Elementary Number Theory and Cryptography,
Easter 2012, Problem Sheet XM.

1. (a) Show or disprove, for p a prime number:
   if $p \mid b$ and $p \mid b^2 + c^2$, then $p \mid c$.
   (b) Let b, c be odd, then show that $16 \mid b^4 + c^4 - 2$.
   (c) Show by induction that
   $$21 \mid 4^{n+1} + 5^{2n-1}\,.$$

2. (a) Find $d = \gcd(777, 497)$ and write d as a linear combination of 777 and 497.
   (b) Find the (multiplicative) inverse 17^{-1} in the ring $\mathbb{Z}/101\mathbb{Z}$.
   (c) Show that there are infinitely many primes of the form $6k - 1$.
   (d) (i) Define Riemann's zeta function $\zeta(s)$.
   (ii) State the Riemann Hypothesis.

3. (a) Compute $13^{422} \pmod{31}$.
   [Carefully formulate any result you use.]
   (b) Find a primitive root modulo 19.
   (c) Solve the congruence
   $$x^{17} \equiv 2 \pmod{31}\,.$$

4. (a) (i) Define Euler's φ-function (or "totient" function).
   (ii) Determine $\varphi(3024)$. [Carefully formulate any result you use.]
   (iii) Give a formula for $\varphi(p^r)$ for a prime power p^r $(r > 0)$, and write down a proof for it.
   (b) Give infinitely many solutions, if any, of the simultaneous congruence
   $$x \equiv 15 \pmod{23}$$
   $$x \equiv 7 \pmod{29}\,.$$
   (c) Determine whether the congruence has a solution
   $$x^2 - 3x + 6 \equiv 0 \pmod{107}\,.$$
   (d) Formulate the Discrete Logarithm Problem.
   (e) (i) Given the pair (n, e) with $\gcd(e, \varphi(n)) = 1$, find an inverse to the map $E : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, given by $m \mapsto m^e \pmod{n}$.
   (ii) For the RSA key (n, e) with modulus $n = 187$ and encryption exponent $e = 23$, find a decryption exponent.

5. (a) Define the Legendre symbol for an odd prime p.
   (b) (i) Formulate Gauss's lemma about the Legendre symbol.
   (ii) Use Gauss's lemma to compute $\left(\frac{5}{11}\right)$.
   (c) (i) State the quadratic reciprocity law.
   (ii) Compute the Legendre symbol
   $$\left(\frac{101}{691}\right)\,.$$
   [Justify your steps carefully.]
   (d) Show that, for $p > 3$ prime, one has
   $$6(p-4)! \equiv 1 \pmod{p}\,.$$
   [Carefully formulate any result you use.]